Technical Cybersecurity

Cybersecurity Today: Exploit Kits

Yikes! Exploit kits?

Browser exploitation

- Automated
- Relatively up-to-date
- Hosted on compromised websites

Thriving grey market

- Rig, Angler, Neutrino, Sundown, Disdain, Terror, Magnitude, Grandsoft
- Rig, Magnitude, Grandsoft most active today

How do they work?

Navigate to compromised website

- Wordpress, malvertising networks, etc.

Use your browser

- Compromise browser and then your system
- Pivot from browser to other systems accessible from yours

Who runs these?

Well, criminals, duh.

Who really runs these?

International Criminal Groups

- Provided as malware-as-a-service
- Used by a variety of organizations
- Customer service, dashboard and statistics, etc.

Multiple payload types

- Ransomware, botnets, credential theft, IP theft, etc.

What about advanced threats?